世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6
G06F 15/00, G06K 9/00

A1

(11) 国際公開番号 WO97/31317

(43) 国際公開日 1997年8月28日(28.08.97)

(21) 国際出願番号 PCT/JP96/00424

(22) 国際出願日 1996年2月23日(23.02.96)

(71) 出願人（米国を除くすべての指定国について）
株式会社 日立製作所(HITACHI, LTD.)[JP/JP]
〒101 東京都千代田区神田駿河台四丁目6番地 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
舩橋誠壽(FUNABASHI, Motohisa)[JP/JP]
〒228 神奈川県相模原市新磯野4-6-4-505 Kanagawa, (JP)
仙石浩明(SENGOKU, Hiroaki)[JP/JP]
〒215 神奈川県川崎市麻生区王禅寺320-102 Kanagawa, (JP)
前田 章(MAEDA, Akira)[JP/JP]
〒224 神奈川県横浜市都筑区葛ケ谷7-207 Kanagawa, (JP)
吉田健一(YOSHIDA, Kenichi)[JP/JP]
〒364 埼玉県北本市高尾2-232 Saitama, (JP)
(74) 代理人
弁理士 小川勝男(OGAWA, Katsuo)
〒100 東京都千代田区丸の内一丁目5番1号
株式会社 日立製作所内 Tokyo, (JP)

(81) 指定国 JP, US, 欧州特許 (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

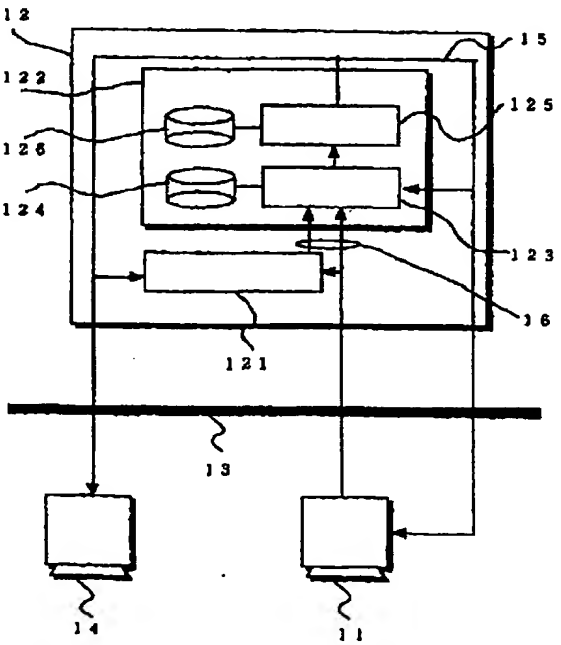
添付公開書類
国際調査報告書

(54)Title: **METHOD FOR CONTROLLING ACCESS TO INFORMATION SYSTEM**

(54)発明の名称 情報システムのアクセス管理方法

(57) Abstract

A method for disclosing a user making fraudulent use of an information system and excluding such a user from the regular use. User authentication is repeatedly performed during a session based on the user's physiological characters and habits when the user operates a terminal and writes a program. This authentication is automatically performed using a learning technique and can follow up frequent change of users and changes of user's habits with time. The access of a user is limited or reported to the system controller in accordance with the degree of qualification of the user obtained as a result of certification. The safety of the information system against fraudulent use can be improved as compared with the conventional method using passwords only. In addition, the system controller can monitor the action of the user one by one and safety control and operate the system without analyzing the disclosed unauthentic user.



（５７）要約

本発明は、情報システムにおいて、不正な利用をしているユーザを摘発するとともに、このユーザを情報システムの利用から排除することを目的とする。

この目的を達成するためにユーザの生理的な特質や端末操作、プログラム動作などの性癖を手がかりにして、ユーザの認証をセッションの最中に繰り返し行う。この認証は、学習技術に基づいて自動的に構築し、ユーザの頻繁な入れ替わりやユーザの性癖の掲示的な変化に追従する。さらに、認証の結果得られるユーザの正当性の度合に応じて、ユーザの行動範囲を制限したり、システム管理者への報告等を行う。

この構成により、従来のパスワードのみによるアクセス管理に比べて、不正利用からの安全性を高めることができる。また、システム管理者は、ユーザの行動を逐一監視でき、不正ユーザの摘出分析をすることなく、安全にシステムを管理、運営できる。

明 細 書

情報システムのアクセス管理方法

技術分野

本発明は、複数のユーザが利用（アクセス）可能な情報システムに係る。この情報システムにおいて、ユーザからのアクセス要求への対応、特にアクセス権限を与えていないユーザからの不正な情報システムの利用を防止するアクセス管理方法に関する。

背景技術

従来の情報システムに対するアクセス管理方法には、予めユーザにパスワードを与えておくものがある。この方法では、ユーザが情報システムへのアクセス開始時に与えられたパスワードを入力し、入力されたパスワードが正当であることが認められた場合に限って情報システムの利用を許すものである。正当なパスワードか否かは、予め与えられたパスワードと入力されたパスワードが同じであり、パスワードを与えられたユーザが、情報システムの利用者として承認されているか否かで判断される。

上述した従来の技術においては、一旦情報システムに対する利用を認めると、ユーザは認められた範囲で自由に情報システムの資源を利用することができる。また、ファイル情報を変更することもできる。

このため、不正行為を働く意志を持った者に情報システムへの利用を許した場合、より厳格に管理がなされているシステム資源への新たなアクセス権利の獲得や、他のユーザの情報システムの利用を妨害できるなどの問題を含んでいる。さらに、情報システムへのアクセス開始時のみ

真のユーザが利用し、それ以外は他のユーザ（アクセスする権利を有しない者）が利用できるとの問題もある。

これらの問題は、以下の①および②により引き起こされる。

①ユーザそれぞれに与えられたパスワードだけを拠り所にしてユーザの認証をしている。

②情報システムへのアクセスの認証を、アクセス開始時にのみ行いそれ以外は全く行っていない。

これらの問題を解決するものが、Teresa F. Lunt著“A survey of intrusion detection techniques, Computers&Security, 12, pp405-418(1993)”に記載されている。これには、ユーザによって引き起こされるプログラムの動作を記録にとり、この記録に対して統計的手法やルールベース手法を適用することが記載されている。この構成により、情報システムを現在利用しているユーザが真のユーザか否かを判断し、不正な情報システムの利用（情報システムへの侵入）を発見する。

しかし、単にプログラム動作に対して統計的手法やルールベース手法を適用するのみでは、十分に不正な情報システムへの侵入を検出することができない。また、この技術では不正な情報システムへの侵入が検出された場合、情報システムの管理者に通報することしかできない。通報するのみでは、情報システムの管理者へ支援を行うための機能が十分発揮されているとは言えない。さらに、不正な侵入に対する検出は集中的に構成されており、情報システムが分散的に構成される今日の情報システムの趨勢を反映していない。

本発明では、情報システムへの不正なアクセスを的確に検出、防止することを目的とする。また、分散的に構成された情報システムに適応する情報システムのアクセス管理方法を提供することも目的とする。さらに、単に不正なアクセスを検出することに止まらず、悪意をもったもの

からの認証機能への攻撃にも強い情報システムのアクセス管理方法を提供することも目的とする。

発明の開示

本発明では、情報システムへのアクセスの認証をパスワードのみに依存しない構成とした。また、認証の作業をただ1度だけでなく、アクセス中（セッション中）に繰り返し行うことにより不正なアクセスを防止する。また、従来不正の検出に用いられていた統計処理やルールベース技術ばかりでなく、より優れた論理をも用いることができるよう全体論理を再構成した。

言い換えれば、ユーザの生理的特徴や端末からの情報システムに対する操作の仕方を認証のための基本情報とし、生体系における免疫作用に関する知見を背景に基本情報に対する判断処理に所定の処理を導入する。また、判断処理機能を情報システム内に存在する1以上の情報処理機構に分散協調的に動作させる構成とした。

ユーザの情報システムに対する操作の仕方や生理的特徴は、ユーザ固有の特徴を表す情報である。ここで、操作の仕方には、端末からの操作パターンなどが考えられる。そして、操作パターンには、端末キーの打鍵の時系列パターン、マウス・ペンの操作時系列パターン、カナ漢字変換などの文字変換パターン、端末から駆動されるファイル生成、ファイル参照・変更パターンなどのプログラム動作パターンなどがある。また、生理的特徴には、顔映像、音声、指紋などがある。

したがって、これらの情報をよりどころとして、セッション中に継続的にユーザの正当性を判断することにより上述した目的を達成できる。正当性とは、例えば、予め登録されたユーザの登録名称と実際にアクセスしているユーザの合致性などを指す。

この正当性の継続的な判断は、非常に不確実な環境下で行わざるを得ない。したがって、本発明においては、必要に応じてユーザの特性を積極的に採取するなど、情報システムの管理上のアクションを判断と並行して行う。

また、情報システム内に存在する１以上の情報処理機構に分散協調的に動作させるためのより具体的な構成は、以下の通りである。それぞれ分散化された管理機能において監視した情報を相互に交換し合い、交換された情報に基づいてアクセス権利の付与を分散的に決定する。

図面の簡単な説明

第１図は、本発明を実現する情報システムの基本構成を示す図である。第２図は、本発明を適用した分散計算機システムの構成を示す図である。第３図は、本発明の運用フローを示す図である。

発明を実施するための最良の形態

以下、本発明の一実施例を説明する。

（１）発明の基本的な構成

第１図は、本発明を実現する情報システムの基本構成を示す。ここで１１は、ユーザが情報システムにアクセスするために用いるユーザ端末である。なお、ここでは１１を１個しか図示しなかったが、１１は１個以上存在する。１２は、ユーザがユーザ端末１１を用いてアクセスし、その資源を活用する情報処理機構である。１２も１１と同様に１個以上存在する。１３は、１１や１２をつなぐ通信ネットワークである。また、１４は情報システムを管理する管理者用のシステム管理者端末１４である。システム管理者端末１４は、必要に応じて設置するよう構成してもよい。

情報処理機構１２は、ユーザからの要求に応じてシステム資源を割り当て、ユーザからの情報処理要求を満たすプロセスモニタ手段１２１とユーザの正当性を判断し状況に応じてしかるべきアクションを発行する繰返し認証手段１２２を有する。ここで、繰返し認証手段１２２は、ユーザの正当性を判断（認証）するユーザ認証手段１２３を有する。ここで、ユーザ認証手段１２３は、格納手段１２４に格納されたユーザ判別関数を用いて正当性を判断する。また、繰返し認証手段１２２は、ユーザ認証手段１２３での判断に基づいてしかるべきアクションを決定し、発行するアクション決定手段１２５も有する。ここで、アクション決定手段１２５は、格納手段１２６に格納されたアクション決定ルールを用いてアクションを決定する。

ここで、ユーザ判別関数とは、ユーザの特徴を表す情報を入力として、そのユーザの正当性を数値として出力する関数である。ここで、ユーザの特徴を表す情報とは、ユーザの情報システムに対する操作の仕方や生理的特徴である。これらについては、上述したものが含まれる。また、操作の仕方は、時系列情報として入力してもよい。

また、アクション決定ルールとは、ユーザ判別関数の出力に基づいて、繰返し認証手段１２２が、システム管理者がとるべき行動の命令を記述したものである。

第１図に示した構成の動作は、以下の通りである。ユーザがユーザ端末１１から情報処理機構１２に対して、まず自分のパスワードを入力して、情報システムを利用する許諾を得る。許諾を得た後、ユーザは、ユーザ端末１１を通して情報処理機構１２に所望の処理を要求する。ここまでは、従来の情報システムにおけるシステム管理のプロセスと同じである。ただし、この処理と並行してユーザ認証手段１２３は、ユーザのユーザ端末１１での操作履歴、ユーザによって引き起こされたプログ

ラムの動作およびユーザ端末１１に装着されたセンサによって測定される生理的特徴のうち少なくとも１つを監視する。そして、ユーザ判別関数を用いて監視された結果が、情報システム側が利用許諾を与えたユーザのものであるかを評価する。

評価する際は、利用許諾を与えるユーザのこれらの特徴を記憶しておき、この記憶内容と監視された結果が同一か否かによって判断する構成もとれる。また、同一の判断においても幅を持たせ、ある程度似ていたら同一と判断する構成もとれる。

さらに、監視は、継続的に行うとより監視の精度があがる。継続的に監視を行うとは、所定時間毎に監視してもよい。また、所定の処理をトリガーとして監視してもよい。また、連続的に監視し続けてもよい。

アクション決定手段１２５は、このように評価された結果を入力として以下の処理を行う。まず、格納手段１２２に格納されたアクション決定ルールに基づいて、情報システムがとるべきアクションを決定し、決定されたアクションに応じて所定の対象にその決定内容を送付する。例えば、現在情報システムを利用しているユーザが正規のユーザか疑わしい場合は、再度キーワードを入力するようユーザ端末１１に表示することがあげられる。また、再度のキーワードの入力がない場合は、情報システムの使用を禁止することもある。

ここで、このようにして使用を禁止されたユーザの特徴を表す情報を記憶しておき、後ほど用いることも考えられる。つまり、このように記憶された情報と監視されたユーザの特徴を表す情報を比較して、比較結果に応じて情報システムの使用を直ちに差し止める。

次にアクション決定手段は、現在ユーザ端末１１を使用しているユーザが、情報システムが本来利用を許しているユーザと異なると判断した場合は、以下の処理を行う。①プロセスモニタに通報して、該当する

ユーザによるプログラムの起動やファイルへのアクセス記録密度を高めたり、これらの行動を制限する。②該当するユーザが利用しているユーザ端末１１に対して、ユーザの正当性を確認するために指定した行動をとるように要請したり、情報システム内における行動を制限する警告を出す。③他の情報処理機構１２に対して、個人認証に不審と見られるユーザが入り込んでいることを通報する。また、そのユーザに関する情報も通報してもよい。ユーザに関する情報とは、例えば、そのユーザの特徴を表す情報や使用しているユーザ端末１１のアドレスなどである。④システム管理者に対して、個人認証に不審とみられるユーザが入り込んでいることを通報する。また、③と同様にユーザに関する情報も通報してもよい。ここで、①～④の処理のうち少なくとも１つをおこなえばよい。

（２）採集すべき情報

ユーザの正当性を繰返し判断するために、本発明では、ユーザの生理的特徴や行動の中でその個人を特徴づける情報を測定する。この測定は、継続的に行うのが望ましい。また、これらの情報は、次にあげるもののみでなく、組み合わせて使用してもよい。

一つは、ユーザがユーザ端末１１を操作する際に測定するものである。言い換えると、ユーザのユーザ端末１１や管理者のシステム管理者端末１２への操作入力に関する時系列情報である。キーボードの打鍵時系列パターン、マウスの動作時系列パターン、仮名漢字変換などの文字変換パターンなどが含まれる。ここで、打鍵時系列パターンには、キーボードを打つ速さ、入力ミス、各キーの使用頻度などのデータが含まれる。マウスの動作時系列パターンには、マウスを動かす速さ、方向、所定時刻の位置などが含まれる。さらに、入力ペンを動かす速さ、方向、所定時刻の位置も含まれる。ここで、文字変換パターンには、アルファベッ

トの大文字小文字変換、異なる言語間での変換（翻訳）も含まれる。以下、これらの情報を端末操作パターンと呼ぶ。

また、端末にカメラやマイクロフォンを付加し、これらを通じて得られる映像情報や音声情報も個人を特徴づける情報である。このほか、指紋を採集すること、腕時計状の装置によってユーザに固有の血流パターンなどの生理学的情報をとり、これを端末に通信する方法もある。

以上述べた打鍵時系列パターンや仮名漢字変換パターンなどには、それぞれ個人固有の特徴が含まれている。本発明では、このことに着目して、これらのパターン（情報）を認証診断に用いるのである。

他の一つは、ユーザ端末１１からの入力によって起動されるプログラムやファイルへのアクセスパターンである。このようなプログラムの実行やファイル生成・参照・変更・消去など一連の履歴情報も、ユーザの個性をあらわす特徴的な情報である。したがって、これらの情報も認証判断処理に活用する。以下、これらの情報をプログラム動作パターンと呼ぶ。

これら二つのタイプの情報は、ユーザ端末１１を利用しているユーザの個性を特徴づけるものである。さらに、継続的に測定可能である。本発明では、これらの情報のいずれか、あるいはその組合わせを個人の認証に用いる。ここで、不正を働く意図をもった者が、これらの情報を奪うおそれがある。これに対して、本発明では、これらの情報を複数のパケットに分散してユーザ端末１１から情報処理機構１２へ送る構成をとってもよい。このとき１人のユーザの特徴情報を複数のパケットに分散してもよい。

次に、具体的な認証判断処理の内容を説明する。

（３）認証判断論理

本発明では、情報システムを利用しているユーザが真のユーザ（アク

セスの権限を与えられたユーザ）なのか、真のユーザになりすましたユーザなのかを調べ、この結果しかるべきアクションをとる認証機能を有する。この際、継続的真のユーザか否かを調べるとより効果的である。

この認証機能を達成するためには、以下の事項を考慮する必要がある。①情報システムが大きくなればなるほど、これを利用するユーザは固定的でなくなる。頻繁なユーザの参入、退去が発生する。②ユーザの情報システムの情報システムの利用における性癖も時間とともに変化する可能性が大きい。

このため、本発明では、システム管理者が認証判断論理の構成に直接手を加えることなく、ユーザの行動パターンなど（ユーザの特徴的な情報）から情報システムが判断論理を学習する構成を採用する。

認証判断論理は、不正なユーザが情報システムの中に入り込んでいるかどうかを検出するものである。また、アクション決定論理は、不正の疑いのあるユーザに対して所定の処置を加えたり、情報システムに対する防御策を講じるものである。なお、アクション決定論理は、認証判断論理の検出内容に従って結論を出すものである。

これらの論理には、生体の免疫作用と同様の機能を持たせる。生体には、自己と非自己とを弁別し、非自己に対しては体内からこれを排除するための攻撃活動を加える。この自己弁別は、遺伝子情報として先天的に組込まれているのではなく、認識細胞が組合せ論的に多様な構成を試行錯誤的にとることによってその作用を達成するようになる。すなわち、生体の弁別の能力は、学習により獲得される。本発明では、生体の免疫作用と同様に学習を行う。以下に、具体的な認証判断論理と学習の仕方を述べる。

本発明では、ユーザの行動パターンや生理的特徴（ユーザの特徴的な情報であり、以下特徴情報と呼ぶ）を生体の免疫系でいう抗原とみなす。

以下、特徴情報をbi(t)であらわすことにする（bi(t)：ユーザｉ（ｉ∈Ｉ）が時刻ｔで示した行動パターンをあらわす特徴情報で、ここには時系列情報も含む）。また、説明のための記号として、ユーザｉが時刻ｔまでに入力した特徴情報の集積（集まり）をBi(t)（＝｛bi(s)｜s∈[t0,t]｝）とあらわす。ここでのt0は、情報システムの動作開始時刻である。なお、ここでの入力は、ユーザが意識せずに情報システムに入力される情報も含む。

本発明では、現在測定している特徴情報が真のユーザである確からしさをあらわす判別関数Ｐ（ｂ，ｗ）を定義し、これを用いて認証判断をする。この判別関数の関数値は、帰属度合を表すものであるが、帰属度合と非帰属度合の二つの値をとるものでもよい。ここに、ｂは特徴情報であり、ｗは判別パラメータである。判別パラメータｗは、ｗｊという値をとり、このパラメータを判別関数に適用したとき、特徴情報ｂのユーザｊへの帰属度合が求められる。すなわち、pij(t)（＝P(bi(t),wj(t))）によって、特徴情報bi(t)が得られたとき、この特徴情報の発信者がユーザｊである確からしさをあらわす。判別パラメータｗｊは、ユーザに固有に識別するものなので、免疫系の抗体に対応するものである。

免疫系では、体内に侵入した抗原に対して特異的に反応する抗体を自己生成する一種の学習論理が備わっている。本発明では、同様の学習論理を備えるため、以下の構成とした。

まず、学習指標Ｌ（ｉ，Ｐ，Ｂ）を定義する。これは、特徴情報の集積Ｂに基づいてユーザｉに関する判別パラメータｗｉを推定するための関数である。すなわち、学習指標Ｌ（ｉ，Ｐ，Ｂ）を最小化する判別パラメータをもってその推定値とする。場合によっては、判別パラメータを再帰的に推定するのが都合の良い場合もある。このために、学習指標

も再帰的に表現する必要があるが、この表現は、L*（i，wi0，P，B）という形をとるものとする。言い換えれば、ユーザiに関する判別パラメータwiを初期推定値wi0から推定する構成としている。

この指標を用いた、時刻tでのユーザiを識別するための判別パラメータwi(t)は以下の通り表すことができる。

wi(t)＝arg min(w){L(i,P(bi',w),bi'∈Bi'(t) for all i')} … (1)

wi(t)＝arg min(w){L*(i,wi0,P(bi',w),bi'∈Bi'(t) for all i')} … (1)'

ここで、arg min(w){}は、変数wに着目して{}内を最小にする項を意味する。この判別パラメータの推定の進行度合を把握する必要があるが、これは次のように定義する学習指標値を用いる。

mi(t)：学習指標値（＝min(x){L(i,P(bi',w),bi'∈Bi'(t) for all i')} もしくは、min(x){L*(i,wi0,P(bi',w),bi'∈Bi'(t) for all i')}

ここで、以上のことを考慮した本発明での学習の仕方は次のようになる。この学習の仕方は、従来の統計的な手法やルールベース手法よりも実現象への適合性がよいという効果を生む。

もし、判別関数として特徴情報を入力として帰属度を出力とするニューラルネットワークによって構成すると、学習指標は出力誤差の自乗値であり、バックプロパゲーションは再帰型表現によるパラメータ推定の論理とみなすことができる。また、判別関数としてファジィルールベースを用いると、判別パラメータはルールに含まれる適合度を定義するパラメータが相当する。この場合、学習指標に基づいて学習するとは、適合度パラメータを最適化することに相当し、この指標としては出力誤差の自乗値をとればよい。

ファジィルールベースは、個人の認証をするのにどんな特徴情報を組み合わせて用いればよいかといった程度の知識がある場合に好都合であ

る。一方、ニューラルネットワークはこのような先見知識が全くない時に有用である。

上記の式（１）および（１）'では最小化操作が含まれているが、種々の特徴情報の組合せを選ぶ場合には、この操作としてランダム探索を含む遺伝的アルゴリズムを採用するとより効果的である。この採用は、判別関数がニューラルネットワークにより構成されようが、ファジィルールベースで構成されようが、特に問題は生じない。

以上、本発明における認証や学習の基本的な枠組みについて述べた。次により具体的に認証や学習を行うかについて述べる。

（ａ）特徴情報の蓄積

ユーザの行動パターンを表す特徴情報は、そのまま蓄積すると厖大な量になってしまう。ここでの特徴情報とは、入力される特徴情報と比較するために情報システムが保持する必要があるもの。このため、データの圧縮をすることが不可欠である。また、認証においてあまり過去の特徴を利用すると、もはや実際に出願しないユーザの性癖（特徴情報）を考慮することになり好ましくない。このため、特徴情報は、一定時間を過ぎたものは廃棄するか、学習に用いないようにする。一定時間としては、予め定めておいてもよい。また、ユーザ毎に変えてもよい。ユーザ毎に変える場合は、各ユーザのアクセス頻度に基づいて定める。

（ｂ）初期学習

ユーザが初めて情報システムにアクセスしようとする際、繰返し認証手段１２２は、入力された特徴情報から認証論理を構築する。このことを初期学習と呼ぶ。これは、学習指標値mi(t)があるしきい値mi０に到達するまでは、集積データから判断パラメータを継続的に学習することを意味する。このプロセスを式に表せば次のようになる。

mi(t0)＝mit０（＝const） t0＝初期時刻

for t>t0

if mi(t)≦mi0(=const'<mit0)

then wi(t)=arg min(w){L(i,P(bi',w)｜bi'∈Bi'(t) for all i')}

& mi(t)=min(w){L(i,P(bi',w)｜bi'∈Bi'(t) for all i')

otherwise do nothing （データの蓄積） … （2）

ここでは、学習指標値を初期時刻には適当な値に設定し、以降の時刻で目標とする指標値mi0に到達するまで学習を繰り返す。式（2）では、再帰型の学習指標を用いてもよい。

もし、ユーザが過去に別の情報処理機構において、繰返し認証手段１２２にアクセスした経験があり、その判別関数が作られている場合には、通信ネットワーク１３を通して判別関数および判別パラメータを複写して当該情報処理機構１２の繰返し認証手段１２２に登録するする。このことにより、初期学習の手間を省くことができる。

（c）認証判断

初期学習が終了した時点で、認証を開始する（ユーザが情報システムにアクセスするのが２度目以降の場合は初期学習無しに）。ユーザｉと称するユーザがユーザｊである確からしさを次のように算出する。

if mi(t)≦mio then pij(t)=P(bi(t),wj(t)) otherwise pij(t)

=null for all i,j … （3）

ここで、nullとは判断パラメータの学習が終了しておらず、判断を保留することを意味する。

（d）追加学習

データの集積の要素数が一定値以上であれば、それまでの判別パラメータ値を初期値として再度パラメータ推定をする。推定結果がよければパラメータ値を更新し、そうでなければそのままとする。すでに、判別パラメータが推定されているのだから、この場合には、再帰型の学習

指標を利用する。これらのプロセスは次のように表現される。

if ∃ i such that mi(t) ≦ mio and Φ ,{ Δ Bi(t',t)(= Bi(t)/Bi(t'), t'<t)}≧α

then if min(w){L*(i,wi(t'),P(bi',w) ¦ bi'∈ΔBi'(t',t) for all i')}

<mi(t')

then wi(t)=arg min(w){L*(i,wi(t'),P(bi',w) ¦ bi'∈ΔBi'(t',t) for all i')}

&mi(t)=min(w){L*(i,wi(t'),P(bi',w) ¦ bi'∈ΔBi'(t',t) for all i')}

oterwise wi(t)=wi(t') & mi(t)=mi(t')

ここで、Φは集合の濃度を表す。

(e) アクション決定

アクション決定手段125では、あらかじめ定めた値域R(n)と判別結果とを照合し、しかるべきアクションを発行する。具体的には、以下の通りである。状況によっては、IF部分に対して、忘却係数をいれた積分的な評価および緊急時における忘却係数調整も行う。

if {{pij(t) ¦ i,j∈I}, {mi(t) ¦ i∈I}}∈R(n) then

アクション番号=n n=1, ..., N … (5)

主要なアクション決定ルールには、次のようなものがある。

(イ) if 学習が十分に進行しており、piiが大、かつpij(i≠j)が小

then 正当なユーザであり、そのままアクセス許容

(ロ) if 学習がやや進行しており、piiが大、かつpij(i≠j)が大 (いずれかのjが)

then 他のユーザと偽っているユーザの可能性が高く緊急体制に入る必要あり

緊急体制としては、「情報システムのシステム管理者に知らせる」

「ユーザが利用を望むシステム資源の利用を制限する」「当該ユーザのシステム利用ログの密度を高める」「当該ユーザに警告を発する」「当該ユーザに特徴情報の入力をうながす」などがある。

（ハ）if　学習がやや進行しており、piiが小、かつpij(i≠j)が小
then　ユーザと認められていない者が情報システムを利用している判断し、緊急体制に入る

並行して、過去のユーザの判別関数、判別パラメータを用いて、ユーザの特定を試みると同時に、このユーザの特徴情報に対する学習を開始する。特に、情報システムの建設に関わった者が不正行為をする事例がしばしばみられる。そこで、情報システムの建設に関与者の判別関数および判別パラメータのうち少なくとも一方を情報システムの建設時に学習し、情報システムの運用時にも活用できるようにしておく。

これらのアクションルールは、ＩＦ～ＴＨＥＮ形式で記述することにより、内容の分かり易さが増し、よりきめ細かな情報システムの管理を支援できる。

（４）分散強調繰返し認証機能

分散計算機では、第２図に示すような構成をとる。各々の繰返し認証手段１２２がお互いに連携して動作する。ここでは、情報システムとして次のような動作モデルを想定する。①複数の情報処理機構１２があり、それぞれの情報処理機構は認証機能を有する繰返し認証手段１２２を備える。②ユーザは、これら複数の情報処理機構１２を渡り歩く。③それぞれの情報処理機構１２の繰返し認証手段１２２は、ユーザがその情報処理機構１２を管理する資源を訪れた時のみ特徴情報を観測できる。

このような分散計算機システムにおいて留意すべき事柄を次にあげる。①情報システム全体として、認証の質をあげるべきである（第１種、第２種の過誤をできるだけ少なくする）。②しかし、このために観測デー

タをすべて交換してしていては、ネットワークにかける負担が大きくなる。したがって、ネットワークに負荷をできるだけかけないで認証の質を高く保つ必要がある。③情報処理機構１２は、保守を受けるために停止したり、新たにシステムに追加されたりする。しかし、各情報処理機構１２で行う認証の質は、できるだけ均質であることが望ましい。あるいは、漸次的に同質になるのが望ましい。

これらに事項を考えて、分散計算機システムでの学習、認証、アクション決定を構成すると次のようになる。

（ａ）分散協調的学習

分散計算機システムにおける認証論理を構成するために、次の記号を定義する。

bi｜k(t)：時刻ｔに、ユーザi(i∈I)が情報処理機構k(k∈K)に入力した特徴情報

Bi｜k(t)：時刻ｔまでに、ユーザi(i∈I)が情報処理機構k(k∈K)に入力した特徴情報の集積（bi｜k(s)｜s≦t)

wi｜k(t)：情報処理機構k（k∈K）が持つユーザｉ（ｉ∈Ｉ）に対する学習指標値

さらに、認証のために情報交換に係わる情報処理機構群１２の状態として次のものを想定する。

送り側の状態＝｛初期学習完了、効果ある追加学習完了｝

受け側の状態＝｛未学習、追加学習中｝

このような想定下に、送り側がなすべきを次にように構成する。初期学習が完了した時点では、推定パラメータをブロードキャストし、未学習の情報処理機構１２を助ける。効果のある追加学習ができた場合には、この追加学習に用いたデータが有用であるとしてブロードキャストするとう考え方である。このことを数式で表現すると次のようになる。

初期学習完了

if ∃i such that mi ¦ k(t)≦mi ¦ ko&mi ¦ k(t')＞mi ¦ ko(for any t'＜t) then broadcast wi ¦ k(t)　… (6)

効果ある追加学習完了

if ∃i such that mi ¦ k(t)≦mi ¦ k(t')(for any t'＜t) then broadcast {ΔBi ¦ k(t) ¦ for all i}　… (7)

一方、受け側の動作は次のようになる。すなわち、未学習時に推定パラメータを受信した場合には、これを初期値として学習を試行する。学習終了段階では、データを受信して追加学習する。このほか、未学習時にデータを受信して、その時点までにもっていたデータと併せて初期学習を試行することも可能である。具体的にこの手順をあらわすと次のようになる。

未学習

if mi ¦ k'(t)＞mi ¦ k'0&wi ¦ k(t) is recieved

then if min(w){L*(i,wi ¦ k(t),P(bi',w) ¦ bi'∈Bi' ¦ k'(t)for all i')}≦mi ¦ k'o

then wi ¦ k'(t)＝arg min(w){L*(i,wi ¦ k(t),P(bi',w) ¦ bi'∈Bi' ¦ k'(t) for all i')}

& mi ¦ k'(t)＝min(w){L*(i,wi ¦ k(t),P(bi',w) ¦ bi'∈Bi' ¦ k'(t) for all i')}　… (8)

追加学習

if mi ¦ k'(t)≦mi ¦ k"0&{ΔBi ¦ k(t) ¦ for all i} is recieved

then if min(w){L*(i,wi ¦ k'(t),P(bi',w) ¦ bi'∈ΔBi' ¦ k'(t)for all i')}＜mi ¦ k'(t)

then wi ¦ k'(t)＝arg min(w){L*(i,wi ¦ k'(t),P(bi',w) ¦ bi'∈ΔBi" ¦ k'(t) for all i')}

& mi ¦ k'(t) = min(w) {L*(i, wi ¦ k'(t), P(bi', w) ¦ bi' ∈ ΔBi" ¦ k'(t) for all i')} … (9)

このように、分散計算機システムにおいて、学習論理を分散協調的に構成することにより、一つの情報処理機構では、成し遂げられなかった精度の高い認証論理を構築可能となる。

（b）分散協調的認証およびアクション決定

第２図に示すような分散計算機システムの各々の情報処理機構１２での認証、アクション決定は、先に述べた分散強調学習論理によって各情報処理機構１２が獲得した判別パラメータを各々がおこなえばよい。この場合に、各情報処理機構１２が相互に干渉するアクションを発行した方が適切なことがある。

たとえば、ある情報処理機構で、正当性の低いユーザの存在が検出された場合を想定してみる。このような場合、単にそのアクションを自己の情報処理機構の範囲に留めておくよりも、他の情報処理機構に通報した方が安全性が高める。また、このような報告を他の情報処理機構から受信した場合は、自己の情報処理機構に対して報告に応じた対応措置をとる。対応措置としては、通報されたユーザに対してはアクセスを禁止することなどがある。

このため、分散計算機システムにおいては、式（５）で述べたアクション決定ルールとしては、学習指標値の高い判別関数値を持つもの（予め基準を定めておきそれよりも学習指標値の高いもの）をマージして判別結果を求め、この結果をアクション決定に結び付ける、といった形のものとする。

たとえば、他人になりすましたユーザが検出された場合には、このことを他の情報処理機構に伝える。また、このような報告が他の情報処理機構から送られてきた場合には、自己の判断にこの報告を勘案して、そ

のアクションを決定する。このようなマージ処理により、情報システム全体としてのユーザの挙動の判断、対応措置を的確に行えるようになる。

（５）アクセス管理の全体動作

以上述べたアクセス管理の全体動作をまとめると第３図のようになる。ユーザは、情報システム利用の申請を所定の手順に従って行う。情報処理機構１２は、ユーザの性癖（ユーザを特定する情報）を学習するまでは、情報処理機構１２自身の持つ資源のうち所定のもの限定して利用を許諾する。例えば、全ての人間に解放しても問題のない公的な資源などのみに限定して利用を許諾する。情報処理機構１２が、ユーザの性癖を学習した段階で、資源の活用を解放する。この資源の活用もユーザによって多段階的に解放する構成もある。また、資源の解放の他に情報処理機構は、ユーザの正当性を認証し、必要に応じて資源解放の範囲を制限する。ここで、ユーザの正当性の認証は、継続的行ってもよい。

産業上の利用可能性

本発明によれば、情報システムにアクセスしている者（ユーザ）をその動作特性のレベルで監視しているので、情報システムにおける不正な行為を抑止できる。さらに、本発明のアクセス管理方法は、分散協調的に行うことができるので、不正な攻撃や予期しない情報システムの部分故障に対しても非常に強靭である。

以上の通り、本発明は、情報システムの安定的な管理に適したものである。

請 求 の 範 囲

1．入力された情報に対して所定の処理を施す複数の情報処理機構と、前記情報処理機構での処理を実行させるための情報を入力可能な複数の端末と、前記情報処理機構および前記端末を結合するネットワークからなる情報システムにおいて、

予め前記システムに蓄えられた所定の資源を利用可能な者の個性を表す特徴情報を記憶しておき、

前記端末を操作している操作者の個性をあらわす特徴情報を反復的に取り込み、

前記取り込んだ特徴情報および前記記憶された特徴情報から反復的に前記操作者が利用を望む資源の利用可能な者である確からしさを求め、

求められた確からしさに応じて前記情報システムの動作を変更することを特徴とする情報システムのアクセス管理方法。

2．請求の範囲第1項に記載の情報システムのアクセス管理方法において、

前記確からしさは、前記取り込んだ特徴情報および前記記憶された特徴情報から判別関数を用いて求めることを特徴とする情報システムのアクセス管理方法。

3．請求の範囲第2項に記載の情報システムのアクセス管理方法において、

前記判別関数の関数構造を予め定めておき、

前記取り込んだ特徴情報を用いて前記判別関数のパラメータを変更することを特徴とする情報システムのアクセス管理方法。

4．請求の範囲第2項または第3項に記載の情報システムのアクセス管理方法において、

前記判別関数は、前記操作者が利用を望む資源の利用可能な者である確からしさおよび前記操作者が利用を望む資源の利用不可能な者である確からしさを求めることを特徴とする情報システムのアクセス管理方法。

5．請求の範囲第１項乃至第４項のいずれかに記載の情報システムのアクセス管理方法において、

前記各情報処理機構間で前記取り込んだ特徴情報を互いに交換し、

前記確からしさを求める際は、前記交換された特徴情報も用いることを特徴とする情報システムのアクセス管理方法。

6．請求の範囲第１項乃至第５項のいずれかに記載の情報システムのアクセス管理方法において、

前記取り込む特徴情報は、前記操作者の前記端末への操作入力に関する時系列情報および前記操作者の操作により引き起こされる前記情報処理機構に格納された情報の動作の時系列情報のうち少なくとも一方を含むことを特徴とする情報システムのアクセス管理方法。

7．請求の範囲第１項乃至第６項に記載の情報システムのアクセス管理方法において、

前記操作入力の時系列情報として、予め前記端末に設置したセンサから取り込まれる前記操作者の生理的な特徴を含むことを特徴とする情報システムのアクセス管理方法。

8．請求の範囲第１項乃至第７項のいずれかに記載の情報システムのアクセス管理方法において、

１人の操作者に関する前記取り込む特徴情報が複数ある場合は、前記複数の特徴情報を２以上のパケットとして、前記ネットワークを通して前記情報処理機構に送ることを特徴とする情報システムのアクセス管理方法。

9．請求の範囲第１項乃至第８項のいずれかに記載の情報システムのア

クセス管理方法において、

前記確からしさは、前記情報処理機構の１つが求め、

前記求めた情報処理機構は、他の情報処理機構に求めた結果を前記ネットワークを通して送ることを特徴とする情報システムのアクセス管理方法。

１０．請求の範囲第１項乃至第９項のいずれかにに記載の情報システムのアクセス管理方法において、

前記特徴情報の取り込みは、所定時間毎に行うことを特徴とする情報システムのアクセス管理方法。

１１．請求の範囲第１項乃至第１０項いずれかに記載の情報システムのアクセス管理方法において、

前記情報システムの動作を変更として、前記確からしさの程度に応じて、前記操作者が望む資源に対する利用に制限をつけることを特徴とする情報システムのアクセス管理方法。

１２．入力された情報に対して所定の処理を施す情報システムにおいて、

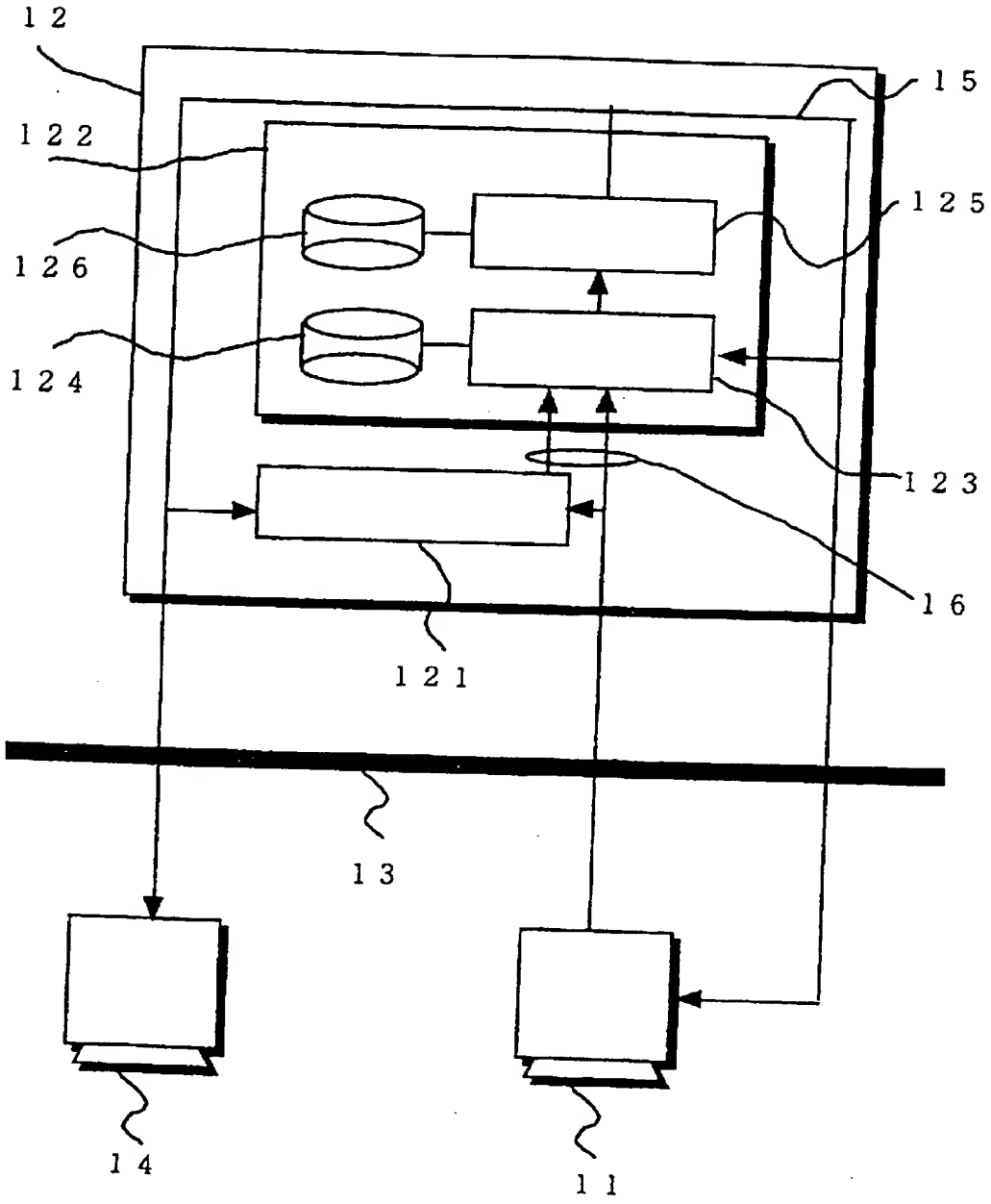
予め前記システムに蓄えられた所定の資源を利用可能な者の個性を表す特徴情報を記憶しておき、

前記情報システムを操作している操作者の個性をあらわす特徴情報を反復的に取り込み、

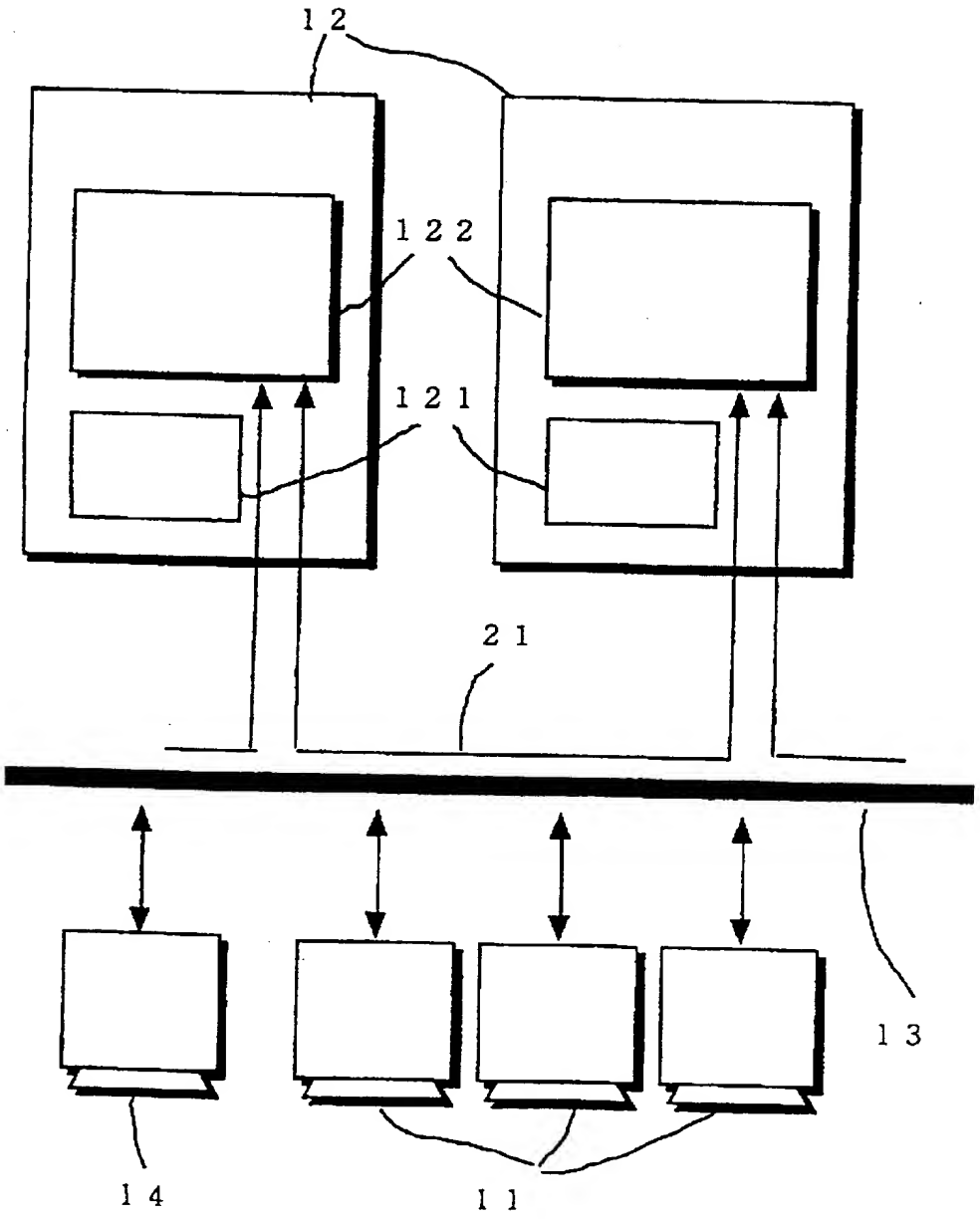
前記取り込んだ特徴情報および前記記憶された特徴情報から反復的に前記操作者が利用を望む資源の利用可能な者である確からしさを求め、

求められた確からしさに応じて前記情報システムの動作を変更することを特徴とする情報システムのアクセス管理方法。

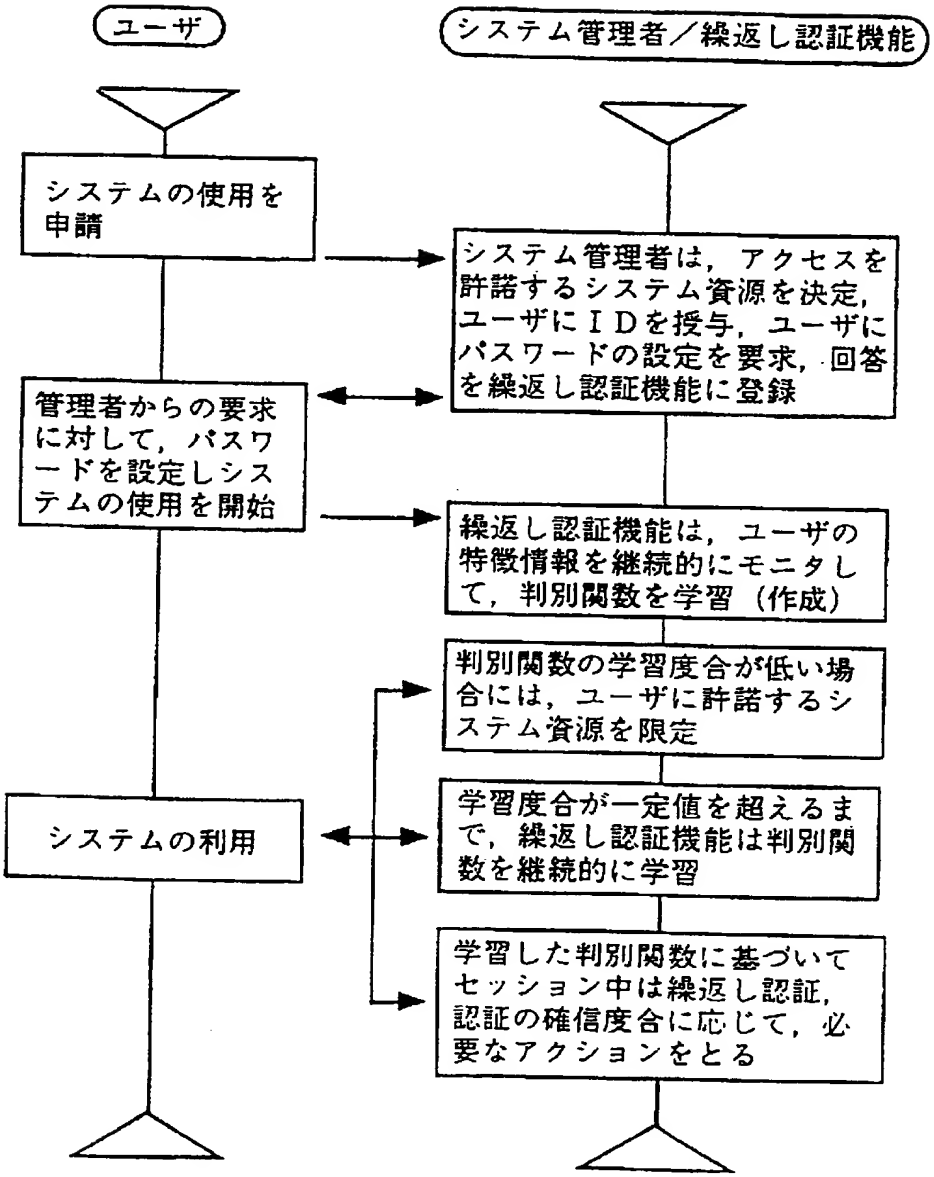
第１図



第２図



第３図


ユーザ
システム管理者／繰返し認証機能
システムの使用を申請
システム管理者は，アクセスを許諾するシステム資源を決定，ユーザにＩＤを授与，ユーザにパスワードの設定を要求，回答を繰返し認証機能に登録
管理者からの要求に対して，パスワードを設定しシステムの使用を開始
繰返し認証機能は，ユーザの特徴情報を継続的にモニタして，判別関数を学習（作成）
判別関数の学習度合が低い場合には，ユーザに許諾するシステム資源を限定
システムの利用
学習度合が一定値を超えるまで，繰返し認証機能は判別関数を継続的に学習
学習した判別関数に基づいてセッション中は繰返し認証，認証の確信度合に応じて，必要なアクションをとる

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP96/00424

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl^6 G06F15/00, G06K9/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
Int. Cl^6 G06F15/00, G06K9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926 - 1996
Kokai Jitsuyo Shinan Koho 1971 - 1996

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 4-311266, A (Applicant), November 4, 1992 (04. 11. 92) (Family: none)	1, 7, 10-12
Y		2, 3, 6, 9
A		4, 5, 8
Y	JP, 5-324805, A (Omron Corp.), December 10, 1993 (10. 12. 93) (Family: none)	2, 3
Y	JP, 5-274269, A (International Business Machines Corp.), October 22, 1993 (22. 10. 93) & EP, 543304, A1	6
Y	JP, 5-257961, A (Applicant), October 8, 1993 (08. 10. 93) (Family: none)	6
Y	JP, 4-342055, A (NEC Corp.), November 27, 1992 (27. 11. 92) (Family: none) (Line 47, left column to line 17, right column,	9

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
May 17, 1996 (17. 05. 96)

Date of mailing of the international search report
May 28, 1996 (28. 05. 96)

Name and mailing address of the ISA/
Japanese Patent Office
Facsimile No.

Authorized officer

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP96/00424

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	page 3)	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP96／00424

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁶　G06F15／00, G06K9／00

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁶　G06F15／00, G06K9／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926－1996
日本国公開実用新案公報　1971－1996

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP, 4－311266, A（出願人） 4. 11月. 1992（04. 11. 92）（ファミリーなし）	1, 7, 10－12
Y		2, 3, 6, 9
A		4, 5, 8
Y	JP, 5－324805, A（オムロン株式会社） 10. 12月. 1993（10. 12. 93）（ファミリーなし）	2, 3
Y	JP, 5－274269, A（インターナショナル・ビジネス・マシンーズ・コーポレイション） 22. 10月. 1993（22. 10. 93）&EP, 543304, A1	6

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」先行文献ではあるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
17. 05. 95	28.05.96

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100 東京都千代田区霞が関三丁目4番3号	徳永民雄　印	5L	9364
	電話番号　03－3581－1101　内線　3564		

様式PCT／ISA／210（第2ページ）（1992年7月）

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ９６／００４２４

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ，５－２５７９６１，Ａ（出願人） ８．１０月．１９９３（０８．１０．９３）（ファミリーなし）	6
Ｙ	ＪＰ，４－３４２０５５，Ａ（日本電気株式会社） ２７．１１月．１９９２（２７．１１．９２）（ファミリーなし） （第３頁左欄第４７行～右欄第１７行）	9